UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,690	02/03/2005	Kazunori Saito	1560-0422PUS1	8523

2292 7590 05/27/2008

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
05/27/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/523,690	SAITO, KAZUNORI	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02-03-05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed 03 February 2005 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because a written English language translation of a non-English language document, or portion thereof (see MPEP § 609.01 [R-5] B,3,b). It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 6 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 6 is directed to a program, *per se*. The body of the claim is directed to the logic steps of the program itself, although, the claim recites memory, no actual structure of the memory is being recited. Furthermore, no actual implementation of the machine/computer is recited into the claim and no actual execution of the program has been implemented. The claim is basically reciting what program steps a program can do. Therefore, it is treated as a program alone.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko (U.S. Pat 6697950 B1) hereinafter referred to as Ko, in view of Bates et al (U.S. Pat Pub 2003/0041315), hereinafter referred to as Bates, as evidenced by Baratloo et al., "Transparent Run-time Defense Against Stack Smashing Attacks," hereinafter referred to as Baratloo.

Re claims 1-7: Ko teaches a data processing method, a computer program (col 3, lines 56-59), including receiving input data containing a plurality of instruction codes (Figs 1 & 2, elt 108; Fig 3, elts 302 & 304; col 4, lines 37-44 and lines 57-63), and judging whether or not a process executed based on the instruction codes contained in the received data is a malicious process (Fig 3, elt 308; col 5, lines 55-61) said method being characterized by comprising:

However, Bates teaches:

retrieving, an instruction code [current statement] related to a branch instruction [Basic Block B] from the data [process] (Fig 5, elts 502 & 504; ¶48, lines 1-19);

storing a branch origin address [blocks reachable from B] associated with the retrieved instruction code and a branch destination address [BRANCHSET] associated with a branch destination of the instruction code (Fig 5, elts 506, 508 & 510; lines 20-26; ¶51, lines 1-30);

judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the branch destination address (Fig 5, elt 508; ¶48, lines 20-26); Bates teaches storing the

storing a call destination address of the instruction code if the instruction code is associated with the branch destination address (Fig 5, elt 508; ¶48, lines 20-26);

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Ko with the teachings of Bates as both references teach tracing through executable code for the purpose of detecting hostile code or instructions. The combination of Ko and Bates is supported by the teachings of Baratloo. Baratloo teaches prevention of “stack smashing”/“buffer overflow” by protecting the stack via canaries (i.e. guards) in the stack; since the stack is used for recalling return addresses and system calls (Abstract; Figs 3, 4 & 5; page 5, right column, ¶3). Analysis of addresses pushed/popped from a program stack is synonymous with tracing through calling/return addresses.

The combination of Ko and Bates teaches judging whether or not the stored call destination address is between the branch origin address and the branch destination address (Ko: Fig 3, elts 304, 306 & 308). The Examiner holds that the branch origin address and branch destination address within a computer program need not have a specific order within a computer program. It is known in the art of computer programming, that function calls could precede the currently executed statement; such practice is common in code which has been obfuscated/scrambled and/or the initial point of execution is obscured as is commonplace in polymorphic and metamorphic code. Ergo, the examiner has interpreted the limitation "judging whether or not the

stored call destination address is between the branch origin address and the branch destination address" to mean analyzing any code in an executable program.

The combination of Ko and Bates teaches the information indicating that the data is data for executing a malicious process is outputted (Ko: Fig 3, elt 310).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

JP 09-128264 A (a translated copy of this document has been included with this Office Action)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2135

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135